I. Vektorräume

§4. Körper, Gruppen, Ringe

4.1| "Körper" sind Mengen, auf denen die 4 Grundrechenarten $\cdot, /, +, -$ definiert sind.

Bsp: a) $\mathbb{Q}$, $\mathbb{R}$ (→ Analysis), $\mathbb{C}$ (s.u.)

b) $\mathbb{F}_2 = \{0,1\}$,

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

−	0	1
0		
1		

$1/1 = 1$.
$0/1 = 0$

c) $\mathbb{Z}$ ist kein Körper, da Division nicht definiert.

4.2| Verknüpfungen

Def: Eine Verknüpfung auf einer Menge M ist eine Abbildung

$$\Phi : M \times M \longrightarrow M.$$

Schreiben wir für $x, y \in M$

$$x \circ y := \Phi(x,y),$$

so heißt Φ

(i) assoziativ, falls $\forall x,y,z \in M \quad (x \circ y) \circ z = x \circ (y \circ z)$

(ii) kommutativ (oder abelsch), falls $\forall x,y \in M \quad x \circ y = y \circ x$.

4.3| Körper

Def: Ein Körper ist eine Menge K mit zwei kommutativen, assoziativen Verknüpfungen "$+$" und "$\cdot$" mit den folgenden Eigenschaften:

(i) $\exists\, 0 \in K : \forall a \in K \quad a+0=0$ (neutrales Element der Addition)

(ii) $\forall a \in K \; \exists\, b \in K : a+b=0$ (additiv Inverses zu a)

(iii) $\exists\, 1 \in K \setminus\{0\} : \forall a \in K \setminus\{0\} \quad a \cdot 1 = a$ (neutrales Element der Mult.)

(iv) $\forall a \in K \setminus\{0\} \; \exists\, b \in K : a \cdot b = 1$ (multiplikativ Inverses zu a)

(v) $\forall a,b,c \in K : a \cdot (b+c) = a \cdot b + a \cdot c$. (Distributivität).

Konventionen: a) Statt $(K, +, \cdot, 0, 1)$ schreiben wir „der Körper K" („Notationsmissbrauch").

b) Punkt- vor Strichrechnung und „$\cdot$" kann man fortlassen. Etwa $a \cdot (b+c) = a \cdot b + a \cdot c$ schreiben wir auch $a(b+c) = ab + ac$.

Bem: a) Die Elemente von K agieren in der "linearen" Algebra als "Skalare". Es wird sich als sehr fruchtbar erweisen, die über $\mathbb{R}$ gewonnene geometrische Intuition auf Situationen über anderen Körpern (z.B. endliche) zu übertragen.

b) Subtraktion und Division reduzieren wir mit (ii) und (iv) zu Addition und Multiplikation:

$a - b = a + c$, wobei c so, dass $b+c=0$ ($c = -b$)

$\frac{a}{b} = a \cdot c$ und c so, dass $a \cdot c = 1$.

4.4 Gruppen

$(K, +, 0)$ und $(K \setminus \{0\}, \cdot, 1)$ sind abstrakt ähnliche Objekte, nämlich „abelsche Gruppen".

Def: Eine **Gruppe** ist eine Menge G mit einer assoziativen Verknüpfung $\circ : G \times G \to G$ mit

(i) $\exists e \in G : \forall a \in G \quad e \circ a = a$. (neutrales Element).

(ii) $\forall a \in G \; \exists b \in G \quad b \circ a = e$. (Inverses zu a)

Ist „$\circ$" kommutativ, so spricht man von einer **abelschen Gruppe**.

Bsp: a) $(\mathbb{Z}, +, 0)$ ist eine abelsche Gruppe

b) $(\mathbb{N} \setminus \{0\}, \cdot, 1)$ ist **keine** Gruppe: $a \in \mathbb{N} \setminus \{0\}$ hat Inverses nur für $a = 1$.

4.5 Exkurs 1: Symmetrische Gruppen: (Bsp. für nichtabelsche Gruppen)

4.5.1

Satz: Für eine Menge M ist

$$Bij(M) := \{ \sigma : M \to M \mid \sigma \text{ bijektiv} \}$$

(Menge der Bijektionen von M auf sich) mit der Hintereinanderausführung von Abbildungen als Verknüpfung

$$\sigma \circ \tau : M \to M, \quad a \longmapsto \sigma(\tau(a))$$

und $e = Id_M$ als neutrales Element, eine Gruppe.

Bew: Neutrales Element: $e = Id_M$.

In der Tat gilt für $\sigma \in Bij(M)$

$$\forall a \in M: \quad (e \circ \sigma)(a) = Id_M(\sigma(a)) = \sigma(a)$$

d.h. $e \circ \sigma = \sigma$.

Inverses Element zu σ: Die Umkehrabbildung σ^{-1}:

$\sigma^{-1}(b)$ = das eindeutige Element $a \in M$ mit $\sigma(a) = b$.

In der Tat gilt:

$$\forall a \in M: \quad (\sigma^{-1} \circ \sigma)(a) = a$$

$$\Rightarrow \quad \sigma^{-1} \circ \sigma = Id_M = e.$$

□

4.5.2| Bsp: $M = \{a, b\}$

$\mathrm{Bij}(M) = \{e, \tau\}$, $\tau: \begin{matrix} a \mapsto b \\ b \mapsto a \end{matrix}$

$\tau^2 := \tau \circ \tau = e$.

Liefert die Multiplikationstabelle

	e	τ
e	e	τ
τ	τ	e

Insbesondere ist $\mathrm{Bij}(M)$ abelsch.

4.5.3| S_n

Ist M endlich, so hängt $S(M)$ bis auf Umbenennung der Elemente ("Isomorphie" s.u.) nur von $\#M$ ab.

Def: $S_n := \mathrm{Bij}(\{1, \dots, n\})$ symmetrische Gruppe auf n Elementen.

Notation für Elemente von S_n: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & & \sigma(n) \end{pmatrix}$.

Etwa: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$1 \longmapsto 2 \longmapsto 3$

$2 \longmapsto 1 \longmapsto 2$

$3 \longmapsto 3 \longmapsto 1$

Dagegen $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Zeigt: S_3 ist nicht abelsch.

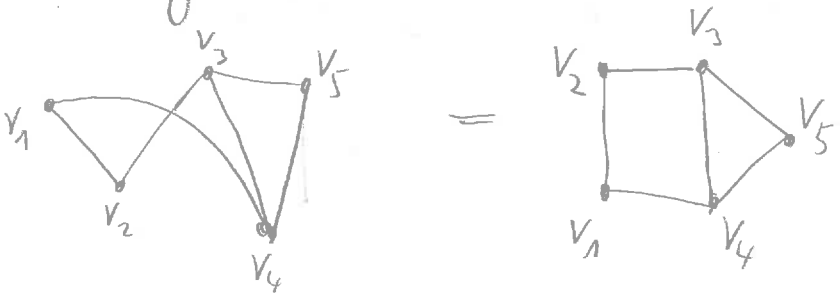
Ähnlich sieht man: S_n ist abelsch nur für $n=2$.

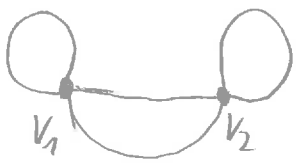
4.6 | Exkurs 2: Symmetriegruppen von Graphen

Ziel: Gruppen & Symmetrien.
Physik: Lorentzgruppe, Spin, Eichtheorien ...

4.6.1 | Graphen – Motivation

Vorstellung: Ein Objekt mit Ecken und Kanten, bei dem nur die "Inzidenzen" wichtig sind.



oder auch  (4 Kanten, 2 Ecken).

Abstraktion: Jede Kante hat 2 Eckpunkte als Enden.
Diese 2 Eckpunkte sind ungeordnet und können sogar übereinstimmen.

$\rightsquigarrow$ 2 Mengen V: Eckpunkte (vertices)
E: Kanten. (edges)

Und für jedes $a \in E$ haben wir Endpunkte $[(v_1, v_2)] \in V \times V / \sim$,

wobei $(v_1, v_2) \sim (v_1', v_2') :\Leftrightarrow$ $v_1 = v_1'$, $v_2 = v_2'$

oder $v_1 = v_2'$, $v_2 = v_1'$.

Demnach $[(v_1,v_2)] = \{(v_1,v_2),(v_2,v_1)\}$. $\left[\#[(v_1,v_2)] = \begin{cases} 1, & v_1=v_2 \\ 2, & \text{sonst} \end{cases}\right]$ (1.7)

Def: Ein (ungerichteter) **Graph** ist ein Paar (V,E) von Mengen zusammen mit einer Abbildung

$$\chi : E \longrightarrow V\times V/\sim .$$

[erlaubt auch isolierte Eckpunkte]

Notation: (V,E,χ)

4.6.2 **Symmetrien**: Bijektionen von V und E auf sich, die die Inzidenzen erhalten. [z.B. ]

Def: Sei $\Gamma = (V,E,\chi)$ ein Graph. Eine **Symmetrie** von Γ ist ein Paar $(\varphi,\psi) \in Bij(V)\times Bij(E)$ mit der Eigenschaft

$$\boxed{\forall a\in E \quad \chi(\psi(a)) = \tilde{\varphi}(\chi(a))} \qquad (*)$$

wobei

$$\tilde{\varphi} : V\times V/\sim \longrightarrow V\times V/\sim, \quad [(v_1,v_2)] \longmapsto [(\varphi(v_1),\varphi(v_2))]$$

die von φ induzierte Abbildung ist. [o.Bew.: $\tilde{\varphi}$ ist wohldefiniert].

Notation: $Sym(\Gamma) = \{\text{Symmetrien von } \Gamma\} \subset Bij(V)\times Bij(E)$.

Satz: $Sym(\Gamma)$ mit $(\varphi,\psi)\circ(\varphi',\psi') := (\varphi\circ\varphi', \psi\circ\psi')$ und $e = (Id_V, Id_E)$ ist eine Gruppe.

Bem: (evtl. fortlassen) Wir müssen zunächst überprüfen, dass $(\varphi\circ\varphi', \psi\circ\psi') \in \mathrm{Sym}(\Gamma)$.

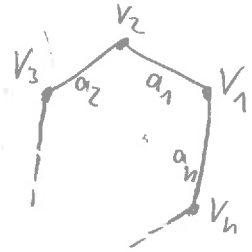
Z: Erfüllen (φ,ψ) und (φ',ψ') Glng. (*), so auch $(\varphi\circ\varphi', \psi\circ\psi')$:

$$\begin{aligned}
\chi((\varphi\circ\varphi')(a)) &= \chi(\varphi(\varphi'(a))) \\
&= \tilde{\varphi}(\chi(\varphi'(a))) && (*) \text{ für } (\varphi,\psi) \\
&= \tilde{\varphi}(\tilde{\varphi}'(a)) && (*) \text{ für } (\varphi',\psi') \\
&= \widetilde{(\varphi\circ\varphi')}(a) && \text{denn } \tilde{\varphi}\circ\tilde{\varphi}' = \widetilde{(\varphi\circ\varphi')}.
\end{aligned}$$

Assoziativität, e: ✓ □

4.6.3 Bsp: Die Diedergruppen

Γ_n = n-Eck, $n \geq 3$



d.h. $V = \{v_1, \dots, v_n\}$, $E = \{a_1, \dots, a_n\}$

$$\chi(a_i) = \begin{cases} [[v_i, v_{i+1}]], & i = 1, \dots, n-1 \\ [[v_n, v_1]], & i = n \end{cases}$$

Def: $D_n := \mathrm{Sym}(\Gamma_n)$ Diedergruppe.

"Offensichtliche" Elemente von D_n:

$\tau = (\varphi,\psi)$, φ: $v_1 \mapsto v_2$, $v_2 \mapsto v_3$, …, $v_{n-1} \mapsto v_n$, $v_n \mapsto v_1$; ψ: $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, …, $a_n \mapsto a_n$ "Drehung"

$\sigma = (\varphi',\psi')$, $\varphi'(v_i) = v_{n+1-i}$, $\psi'(a_i) = \begin{cases} a_{n-i}, & i \neq n \\ a_n, & i = n \end{cases}$ "Spiegelung".

Satz: 1) $D_n = \{e, \tau, \dots, \tau^{n-1}, \sigma, \sigma\tau, \dots, \sigma\tau^{n-1}\}$ und $\# D_n = 2n$

2) $\tau^n = e$, $\sigma^2 = e$, $\sigma\tau\sigma = \tau^{-1}$.

Bem: (2) bestimmt die Gruppenstruktur, wenn man nach $\sigma^i \cdot \sigma^j = \sigma^{[i+j]}$ und $\tau^i \cdot \tau^j = \tau^{[i+j]}$ beachtet.

Bew: (d. Satzes) ↗ Übung. □

4.7| Analyse der Gruppenaxiome

Sei G eine Gruppe. Schreibe ab für $a \circ b$.

4.7.1| Linkskürzung: $\forall a, x, y \in G: \; ax = ay \Rightarrow x = y$.

Bew: Wähle $b \in G$ invers zu a: $ba = e$.

Dann
$$\begin{aligned} x &= ex && (e \text{ neutral}) \\ &= (ba)x && (ba = e) \\ &= b(ax) && (\text{Assoz.}) \\ &= b(ay) && (ax = ay) \\ &= (ba)y && (\text{Assoz.}) \\ &= ey && (e \text{ neutral.}) \\ &= y. \end{aligned}$$

□

4.7.2 | e ist auch rechtsneutral: $\forall a \in G \; ae = a$.

Bew.: Wähle wieder b inverses zu a.

Dann $b(ae) = (ba)e = e \cdot e = e = ba$

$\overset{4.7.1}{\Rightarrow} ae = a$. □

4.7.3 | Satz: (Eindeutigkeit des neutralen Elements.)

Sei $e' \in G$ und

$\forall a \in G \quad e'a = a$.

Dann gilt $e' = e$.

Bew.: $e \overset{(*)}{=} e'e \overset{(4.7.2)}{=} e$ □

4.7.4 | Satz: (Inverse sind beidseitig invers.)

Für $a, b \in G$ gilt:

$ba = e \Rightarrow ab = e$.

Bew.: $b(ab) \overset{(Ass.)}{=} (ba)b = eb = b = be$

$\overset{4.7.1}{\Rightarrow} ab = e$. □

4.7.5 | Rechtskürzung: $\forall a, x, y \in G: \; xa = ya \Rightarrow x = y$

Bew.: analog Linkskürzung.

4.7.6 Satz (Eindeutigkeit der Inversen).

$\forall a,b,c \in G: ba = e,\ ca = e \Rightarrow b = c$

Bew: $ba = e = ca \overset{4.7.5}{\Rightarrow} b = c$ □

Nach 4.7.4 und 4.7.6 ist folgende Konvention sinnvoll:

Notation: Zu $a \in G$ bezeichne $a^{-1} \in G$ das Inverse zu a. Es gilt:

$$a^{-1}a = aa^{-1} = e.$$

4.7.7 Satz: $\forall a \in G \quad (a^{-1})^{-1} = a.$

Bew: $(a^{-1})^{-1} \cdot a^{-1} = e = a \cdot a^{-1}$.

$\overset{4.7.5}{\Rightarrow} \quad (a^{-1})^{-1} = a.$ □

4.7.8 Satz: $\forall a,b \in G: (ab)^{-1} = b^{-1}a^{-1}$

Bew: $(b^{-1}a^{-1}) \cdot (ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e.$ □

4.7.9 Zusammenfassung:

a) Das (linke) neutrale Element ist eindeutig und beidseitig neutral.

b) Linksinverse Elemente sind eindeutig und beidseitig invers.

4.8 Anwendung auf Körper

$(K,+,0)$: additive Gruppe von K.

$(K\setminus\{0\},\cdot,1)$: multiplikative Gruppe von K.

Schreibweise: $a\in K$, dann $-a$ additives Inverses zu a: $a+(-a)=0$.

$a\neq 0$, dann a^{-1} multipl. " " : $a\cdot a^{-1}=1$.

4.8.1 $\forall a\in K: 0\cdot a=0$.

Bew: $0+0\cdot a=0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a$

$\overset{0\cdot a \text{ kürzen}}{\Rightarrow}\quad 0=0\cdot a$. □

4.8.2 $\forall a\in K: (-1)\cdot a=-a$.

Bew: $a+(-1)\cdot a=1\cdot a+(-1)\cdot a=(1+(-1))\cdot a=0\cdot a\overset{4.8.1}{=}0$. □

4.8.3 $\forall a,b\in K: a\cdot(-b)=(-a)b=-ab$.

Bew: $a(-b)+ab=a(-b+b)=a\cdot 0=0$

analog für $(-a)b$. □

4.8.4 $\forall a,b\in K: (-a)\cdot(-b)=ab$

Bew: $(-a)\cdot(-b)\overset{4.8.3}{=}-(-a)\cdot b\overset{4.8.3}{=}-(-ab)\overset{4.7.7}{=}ab$.

□

4.8.5 $\forall a\in K: (-a)^{-1}=-a^{-1}$

Bew: $(-a)\cdot(-a^{-1})\overset{4.8.4}{=}a\cdot a^{-1}=1$.

4.8.6 $ab=0\Rightarrow a=0$ oder $b=0$

Bew: Falls $a\neq 0$, dann

$b=a^{-1}\cdot(ab)=a^{-1}\cdot 0\overset{4.8.1}{=}0$. □

4.9 $\mathbb{Z}/n$ ("Rechnen modulo n").

4.9.1 Teilen mit Rest in $\mathbb{Z}$.

Satz: Sei $n \in \mathbb{N}\setminus\{0\}$ und $a \in \mathbb{Z}$. Dann existieren eindeutige $q, r \in \mathbb{Z}$ mit

$$a = qn + r, \quad 0 \leq r < n.$$

Bew: 1. Zunächst nehmen wir $a \geq 0$ an.

Betrachte $M := \{q \in \mathbb{N} \mid qn \leq a\}$.

Es gilt $M \neq \mathbb{N}$, denn etwa $a+1 \notin M$: $(a+1)n \geq a+1 > a$.

Peano-Axiome $\Rightarrow$ $\exists\, q \in M,\ q+1 \notin M$.

D.h. (I) $qn \leq a$ (II) $(q+1)n > a$

$$\overset{(I)}{\Rightarrow} \quad 0 \leq a - qn \overset{(II)}{<} n.$$

Setze $r := a - qn$.

2. Falls $a < 0$, so gibt es nach (1) $q', r' \in \mathbb{Z}$ mit

$$-a = q'n + r', \quad 0 \leq r' < n.$$

Dann $a = (-q')n - r' = (-q'-1)n + (n-r')$.

Setze

$r' = 0$: $q = -q'$, $r = 0$

$r' \neq 0$: $q = -q'-1$, $r = n - r' \in \{1, \dots, n-1\}$.

3. Eindeutigkeit: $a = qn + r = q'n + r'$ und $0 \leq r, r' < n$.

O.E. sei $q \leq q'$ (sonst q mit q' und r mit r' vertauschen)

Dann gilt $(q'-q)n = r - r' \leq r < n$

Dies ist nur möglich, falls $q'-q=0$, d.h. $q=q'$.

Dann aber auch $r-r'=0$, d.h. $r=r'$. □

Schreibweise: $a \bmod n$ bezeichnet das eindeutige $r \in \{0,\dots,n-1\}$ aus dem Satz mit $a = qn + r$ für ein $q \in \mathbb{Z}$.

4.9.2 Rechnen modulo n

Auf $\mathbb{Z}/n := \{0,\dots,n-1\}$ definieren wir: "$\mathbb{Z}$ modulo n"

Addition: $a +_n b := (a+b) \bmod n$

Multiplikation: $a \cdot_n b := (a \cdot b) \bmod n$.

Bsp: $n=4$. $2 +_4 3 = 1$

$2 \cdot_4 2 = 0$.

Man überprüft leicht, dass $(\mathbb{Z}/n, +_n, \cdot_n)$ die Körperaxiome 4.3 (i), (ii), (iii) und (v) erfüllt, im allgemeinen (d.h. nicht für alle n und a) aber nicht (iv). Ein derartiges Objekt heißt Ring. Auch $(\mathbb{Z}, +, \cdot)$ ist ein Ring, nicht jedoch $(\mathbb{N}, +, \cdot)$.

Bem.: Sind $a, b \in \mathbb{Z}$, so schreibt man statt

$$a \bmod n = b \bmod n$$

auch $a \equiv b \mod n$ "a kongruent b modulo n".

4.9.3 Interpretation als Quotientenmenge

Auf $\mathbb{Z}$ betrachte die Äquivalenzrelation ($n=2 \rightarrow$ Bsp. 3.2,b):

$$a \sim_n b :\Leftrightarrow \exists q \in \mathbb{Z} \quad b = a + qn$$
$$[\Leftrightarrow \quad a \equiv b \mod n.]$$

Äquivalenzklassen: $[a] = a + \mathbb{Z}n = \{a + qn \mid q \in \mathbb{Z}\}$.

"+" und "·" induzieren Verknüpfungen "+" und "·" auf $\mathbb{Z}/n$ mit

$$[a] + [b] = [a+b]$$
$$[a] \cdot [b] = [a \cdot b].$$

Die kanonische Abbildung

$$\Phi: \mathbb{Z}/n \longrightarrow \mathbb{Z}/\sim_n, \quad a \longmapsto [a]$$

ist dann bijektiv (Bew!), und es gilt

$$\forall a, b \in \mathbb{Z}/n \qquad \Phi(a+b) = \Phi(a) + \Phi(b),$$
$$\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b)$$
$$\Phi(1) = 1.$$

Bis auf Umbenennung der Elemente sind also $\mathbb{Z}/n$ und $\mathbb{Z}/\sim_n$

der gleiche Ring. (Φ ist ein Ringisom. ↗5.5)

4.9.4| $\mathbb{F}_p$

Def: Eine Primzahl ist ein $p \in \mathbb{N} \setminus \{0,1\}$ mit

$p = ab$ für $a,b \in \mathbb{N} \Rightarrow a=1$ oder $b=1$.

Satz: Ist p prim, so ist $\mathbb{F}_p := (\mathbb{Z}/p, +_p, \cdot_p)$ ein Körper.

Bew: Später (↗ Euklidischer Algorithmus).

Man zeigt:

$\forall a \in \mathbb{Z} \setminus \mathbb{Z}p \; \exists b,q \in \mathbb{Z}: \; 1 = qp + ab$.

Dann $ab \equiv 1 \mod p$, d.h. $b \bmod p = (a \bmod p)^{-1}$ in $\mathbb{Z}/p$. □

Bsp: $p=3$: $2^{-1} = 2$ $(2 \cdot 2 = 4 \equiv 1 \mod 3)$

$p=5$: $2^{-1} = 3$ $3^{-1} = 2$ $(2 \cdot 3 = 6 \equiv 1 \mod 5)$

$4^{-1} = 4$

$p=7$: $2^{-1} = 4$ $4^{-1} = 2$

$3^{-1} = 5$ $5^{-1} = 3$

$6^{-1} = 6$

Bem: Für jede Primzahlpotenz p^r gibt es einen bis auf Umbenennung der Elemente eindeutigen Körper mit p^r Elementen.

Galoiskörper $\mathbb{F}_{p^r}$.

§5 Homomorphismen

Zwischen Mengen mit Verknüpfungen (Gruppen, Ringe, Körper, ...) sind Abbildungen besonders nützlich, die verträglich mit den gegebenen Strukturen sind. Solche Abbildungen nennt man Homomorphismen.

5.1 Gruppenhomomorphismen

Def: Seien $(G, \circ_G)$ und $(H, \circ_H)$ Gruppen. Eine Abbildung

$$f: G \to H$$

heißt **Homomorphismus**, falls

$$\forall x, y \in G \quad f(x \circ_G y) = f(x) \circ_H f(y).$$

Ist f { bijektiv / injektiv / surjektiv }, so spricht man von einem { Isomorphismus / Monomorphismus / Epimorphismus }.

Bem: a) $f(e_G) = f(e_G \circ e_G) = f(e_G) \circ f(e_G) \Rightarrow f(e_G) = e_H$. b) $f(x^{-1}) = f(x)^{-1}$: ...

5.2 Bsp

a) $f: (\mathbb{Z}/n, +_n) \to (\mathbb{Z}/\sim_n, +)$ aus 4.9.3 ist ein Isomorphismus.

b) $f: (\mathbb{Z}, +) \to (\mathbb{Z}/n, +_n)$, $a \mapsto a \bmod n$ ist ein Epimorphismus.

c) $f: (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ Homom., dann $f(a) = f(\underbrace{1 + \ldots + 1}_{a\text{-mal}}) = \underbrace{f(1) + \ldots + f(1)}_{a\text{-mal}} = a \cdot f(1)$.
D.h. f ist bestimmt durch $f(1) \in \mathbb{Z}$.

d) Sei G eine Gruppe, $g \in G$.
Für $n \in \mathbb{Z}$ definiere

$$g^n := \begin{cases} \underbrace{g \circ \dots \circ g}_{n\text{-mal}}, & n > 0 \\ e, & n = 0 \\ \underbrace{g^{-1} \circ \dots \circ g^{-1}}_{(-n)\text{-mal}}, & n < 0 \end{cases}.$$

Für $n, m \in \mathbb{Z}$ gilt $g^{m+n} = g^m \circ g^n$: (Erfordert Fallunterscheidung.

Etwa für $m < 0$, $n > 0$: $g^m \circ g^n = \underbrace{g^{-1} \circ \dots \circ g^{-1}}_{(-m)\text{-mal}} \circ \underbrace{g \circ \dots \circ g}_{n\text{-mal}} = g^{n-|m|} = g^{n+m}$.
$n+m = n-|m| \geq 0$

Demnach ist

$$f : (\mathbb{Z}, +) \longrightarrow G, \quad n \longmapsto g^n$$

ein Homomorphismus. Jeder Hom. $f : (\mathbb{Z}, +) \to G$ ist von dieser Form ($g = f(1)$).

e) $f : (\mathbb{Z}, +) \to (\mathbb{Q} \setminus \{0\}, \cdot)$, $n \longmapsto a^n$ ein Monomorphismus.
für $a \in \mathbb{Q} \setminus \{0\}$ ist (Spezialfall von (d) mit $g = a$!)

f) Für $m \leq n$ und $\sigma \in S_m$ definiere $\tilde{\sigma} \in S_n$

$$\tilde{\sigma} \in S_n, \quad \tilde{\sigma}(i) = \begin{cases} \sigma(i), & 1 \leq i \leq m \\ i, & m+1 < i \leq n. \end{cases}$$

Dann ist $\iota : S_m \to S_n$, $\sigma \longmapsto \tilde{\sigma}$ ein Monomorphismus.

5.3 Untergruppen

[Bem: Unterobjekte einer algebraischen Struktur].

Def: Sei G eine Gruppe. Eine Teilmenge $U \subset G$ heißt Untergruppe, falls

(i) $e \in U$

(ii) $\forall x,y \in U: x \circ y \in U$ (Abgeschlossenheit unter "$\circ$"),

(iii) $\forall x \in U: x^{-1} \in U$ (" unter $x \mapsto x^{-1}$).

Bsp: a) $n \in \mathbb{Z}$, so ist $n\mathbb{Z} \subset (\mathbb{Z},+)$ eine Ugpp.

b) $f: G \to H$ Homom. $\Rightarrow$ $\mathrm{im}(f) \subset H$ Ugpp:

(i) $e_H = f(e_G) \in \mathrm{im}(f)$.

(ii) $x,y \in \mathrm{im}(f) \Rightarrow \exists a,b \in G: x = f(a), y = f(b)$

$\Rightarrow x \circ y = f(a) \circ f(b) = f(a \cdot b) \in \mathrm{im}(f)$.

(iii) $f(a)^{-1} = f(a^{-1})$: ↗ S.1, Bem.

[In (a) ist $n\mathbb{Z} = \mathrm{im}(f)$, für $f: \mathbb{Z} \to \mathbb{Z}$, $f(a) = an$].

5.4 Kerne

Def: Sei $f: G \to H$ ein Homom. von Gruppen. Dann heißt

$$\ker(f) := \{x \in G \mid f(x) = e_H\}$$

der Kern von f.

Bsp: $f: \mathbb{Z} \to \mathbb{Z}_n$, $a \mapsto a \bmod n$. $\ker(f) = n\mathbb{Z}$.

(1.20)

Satz: Ist $f: G \to H$, so ist $\ker(f) \subset G$ eine Untergruppe.

Ferner gilt:

f injektiv $\iff \ker(f) = \{e\}$.

$\ker(f) \subset G$ Uppp: ✓.

Bew: „$\Rightarrow$": $f(x) = e_H = f(e_G)$

f injektiv $\Rightarrow x = e_G$.

„$\Leftarrow$": $f(x) = f(y)$

$$\Rightarrow e_H = f(e_G) = f(x \circ x^{-1}) = f(x) \circ f(x^{-1}) \overset{\text{Vor.}}{=} f(y) \circ f(x^{-1}) = f(y \circ x^{-1})$$

$\ker(f) = \{e\}$

$\Rightarrow y \circ x^{-1} = e_G$

$\Rightarrow y = x$. □

5.6 Ring- und Körperhomomorphismen

Def: Eine Abbildung $f: R \to S$ zwischen Ringen (Körpern) heißt (Ring-/Körper-) Homomorphismus, falls

(i) $f(1_R) = 1_S$

(ii) $f: (R,+) \to (S,+)$ ist Homom. von Gruppen.

(iii) $\forall x,y \in R: f(x \cdot y) = f(x) \cdot f(y)$.

Satz: Ist K ein Körper, so ist jeder Ringhomom. $f: K \to R$ injektiv.

Bew: Wir zeigen: $\ker(f) = \{0_K\}$: $x \in \ker(f) \setminus \{0\} \Rightarrow 1_R = f(1_K) = f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$

$\Rightarrow f(x) \neq 0_R$.

Bem: Körpererweiterungen, Teil-/Unterkörper, etwa $f: \mathbb{Q} \to \mathbb{R}$.

1.21 1/2

Cardano: Ars magna sive de regulis algebraicis 1545

Finde a, b mit $a+b=10$, $a \cdot b = 40$

$\rightsquigarrow$ $x(10-x) = 40$

$x^2 - 10x + 40 = 0$

$x = \frac{10 \pm \sqrt{100-160}}{2}$

$= 5 \pm \sqrt{-15}$

"So schreitet der arithmetische Scharfsinn voran, der ebenso subtil wie nutzlos ist".

→ Formel von Cardano für NST von $ax^3 + bx^2 + cx + d$. (→ del Ferro, Tartaglia)

- Cardanische Aufhängung
- Das Buch der Glücksspiele (→ W-theorie)

§6. Komplexe Zahlen

In $\mathbb{R}$ ist das Quadrat jeder Zahl größer oder gleich 0. Insbesondere hat die Gleichung

$$x^2 = -1$$

keine Lösung. Wir beheben dies durch Erweiterung von $\mathbb{R}$ zu $\mathbb{C}$ durch Einführung eines neuen Elements i, der "imaginären Einheit", mit der Eigenschaft $i^2 = -1$. Für $\lambda, \mu \in \mathbb{R}$ sind dann auch $\lambda + i\mu \in \mathbb{C}$.

6.1 Algebraische Definition von $\mathbb{C}$

Geschichte: → Cardano

Idee: Schreibe $\lambda + \mu i$ als Paar (λ, μ), d.h. def. als Menge $\mathbb{C} := \mathbb{R} \times \mathbb{R}$.

Die formalen Rechnungen:

$$(\lambda + \mu i) + (\lambda' + \mu' i) = (\lambda + \lambda') + (\mu + \mu')i$$

$$(\lambda + \mu i) \cdot (\lambda' + \mu' i) = \lambda\lambda' + \lambda\mu' i + \mu\lambda' i + \mu\mu' i^2 \qquad (*)$$
$$= (\lambda\lambda' - \mu\mu') + (\lambda\mu' + \mu\lambda')i$$

motivieren die folgende Def.

Def: Der Körper $\mathbb{C}$ der komplexen Zahlen ist die Menge $\mathbb{R} \times \mathbb{R}$ mit den Verknüpfungen $+$ und $\cdot$ mit

$$(\lambda, \mu) + (\lambda', \mu') := (\lambda + \lambda', \mu + \mu')$$

$$(\lambda, \mu) \cdot (\lambda', \mu') := (\lambda\lambda' - \mu\mu', \lambda\mu' + \mu\lambda').$$

Schreibweise: $i := (0,1)$ und $\lambda+\mu i := (\lambda,\mu)$, $\lambda = (\lambda,0)$, $\mu i = (0,\mu)$ (Multiplikation (*))
$= \lambda + i\mu$

6.2| Satz: $(\mathbb{C},+,\cdot)$ ist ein Körper mit $0 := 0+0i$, $1 := 1+0i$.

Bew: 1) $(\mathbb{C},+,0)$ ist eine komm. Gruppe:

Dies folgt komponentenweise aus der nämlichen Eigenschaft von $\mathbb{R}$.

2) $(\mathbb{C}\setminus\{0\},\cdot,1)$ ist eine komm Gruppe:

Einheit: $(1+0\cdot i)\cdot(\lambda+\mu i) = \lambda+\mu i$.

Assoziativität: $(\lambda+\mu i)\cdot\big((\lambda'+\mu' i)\cdot(\lambda''+\mu'' i)\big) = \dots$

$$= (\lambda\lambda'\lambda'' - \lambda\mu'\mu'' - \lambda'\mu\mu'' - \lambda''\mu\mu') + (\lambda\lambda'\mu'' + \lambda\lambda''\mu' + \lambda'\lambda''\mu - \mu\mu'\mu'')i$$

$$= \dots = \big((\lambda+\mu i)(\lambda'+\mu' i)\big)\cdot(\lambda''+\mu'' i),$$

Inverse: Zu $\lambda+\mu i \neq 0$ ist $\frac{\lambda}{\lambda^2+\mu^2} - \frac{\mu}{\lambda^2+\mu^2}i$ Inverses!

$$(\lambda+\mu i)\cdot\left(\frac{\lambda}{\lambda^2+\mu^2} - \frac{\mu}{\lambda^2+\mu^2}i\right) = \frac{\lambda^2+\mu^2}{\lambda^2+\mu^2} + \frac{-\lambda\mu+\lambda\mu}{\lambda^2+\mu^2}i = 1$$

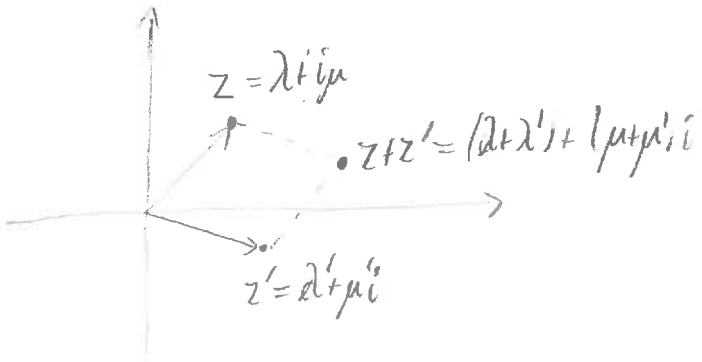
3) Distributivität: Rechnung! □

Bsp: $(3+4i)^{-1} = \frac{3-4i}{3^2+4^2} = \frac{3}{25} - \frac{4}{25}i$.

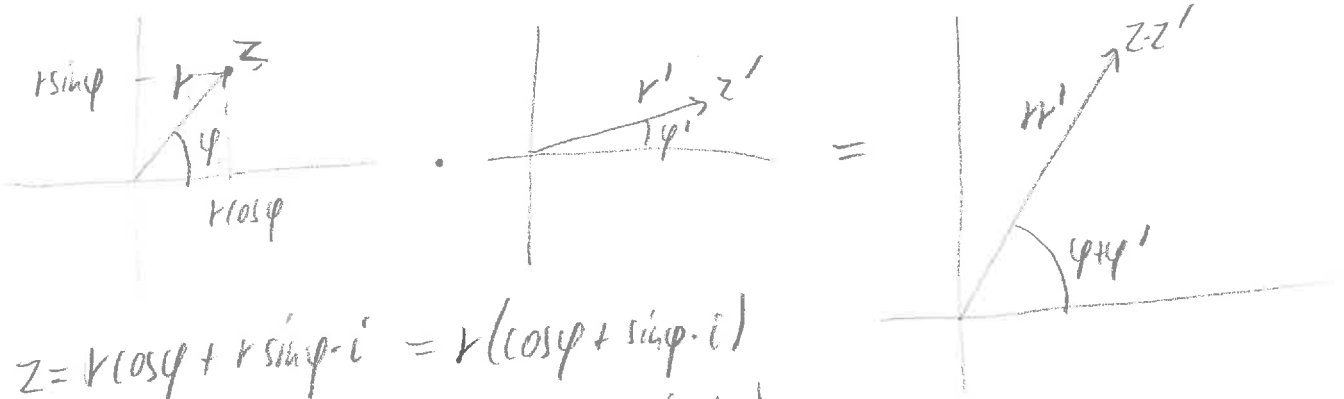
6.3 Die Gaußsche Zahlenebene

Visualisiere komplexe Zahlen als Punkte in der Zahlenebene.

Addition $\leftrightarrow$ Summe von Vektoren:



Multiplikation: Multipliziere Länge der Vektoren, addiere Winkel zur x-Achse.



$z = r(\cos\varphi + \sin\varphi \cdot i) = r\cdot e^{i\varphi}$

$z' = r'(\cos\varphi' + \sin\varphi' \cdot i) = r'\cdot e^{i\varphi'}$.

$$z\cdot z' = rr'(\cos\varphi\cos\varphi' - \sin\varphi\sin\varphi') + rr'(\cos\varphi\sin\varphi' + \sin\varphi\cos\varphi')\cdot i$$

$$= rr'\cos(\varphi+\varphi') + rr'\sin(\varphi+\varphi')\cdot i \quad \left(\text{Additionstheoreme} \rightsquigarrow \text{Anal.}\right) \;//$$

Anwendung: Drehung um 90° = Multiplikation mit i.

6.4 Realteil, Imaginärteil, Betrag, komplexe Konjugation

Def: Zu $\lambda+i\mu \in \mathbb{C}$ definiere

$\mathrm{Re}(\lambda+\mu i) := \lambda$ Realteil;

$\mathrm{Im}(\lambda+\mu i) := \mu$ — Imaginärteil

$\overline{\lambda+\mu i} := \lambda-\mu i$ — komplex Konjugierte

$|\lambda+\mu i| := \sqrt{\lambda^2+\mu^2} = \sqrt{z\bar{z}}$ — Betrag / Länge.

insbes. $\lambda \in \mathbb{R}_{\geq 0}$: $|\lambda z| = \lambda \cdot |z|$.

Demnach: $z \in \mathbb{C}\setminus\{0\}$, dann $z^{-1} = \frac{\bar{z}}{z\bar{z}} = \frac{\bar{z}}{|z|^2}$. Bem: a) $|zw| = |z|\cdot|w|$.

b) $z \in \mathbb{R} \Leftrightarrow z = \bar{z}$

$\overline{zw} = \bar{z}\cdot\bar{w}$

6.5 Polardarstellung, Eulersche Formel

Für $\varphi \in \mathbb{R}$ schreibe $\boxed{e^{i\varphi} := \cos\varphi + i\sin\varphi}$ Eulersche Formel

[Motiviert durch Einsetzen von $i\varphi$ in die Exponentialreihe $\nearrow$ Analysis].

Analysis: $z \in \mathbb{C}$, $|z|=1 \Leftrightarrow \exists!\, \varphi \in [0,2\pi)$ mit $z = \cos\varphi + i\sin\varphi$. (vgl. 6.3)
$= e^{i\varphi}$

Für allgemeine $z \in \mathbb{C}\setminus\{0\}$: $\left|\frac{z}{|z|}\right| = \frac{1}{|z|}|z| = 1$

$\Rightarrow \exists \varphi \in [0,2\pi) : z = |z| e^{i\varphi}$.

Polardarstellung von z: $\boxed{z = r e^{i\varphi}}$.

Argument von $z \neq 0$: $\mathrm{Arg}(z) := \varphi \in [0,2\pi)$. (oder: $\in \mathbb{R}/2\pi\mathbb{Z}$)

Bem: $(re^{i\varphi})\cdot(r'e^{i\varphi'}) = rr'\cdot e^{i(\varphi+\varphi')}$.

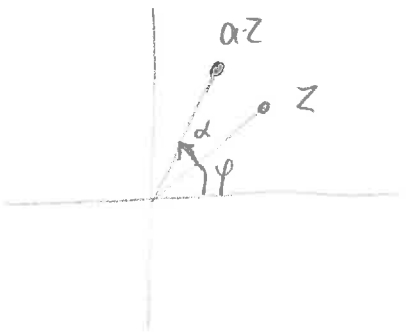
Demnach $\mathrm{Arg}(zz') = \begin{cases} \mathrm{Arg}(z)+\mathrm{Arg}(z'), & \text{falls } < 2\pi \\ \mathrm{Arg}(z)+\mathrm{Arg}(z')-2\pi, & \text{falls } > 2\pi. \end{cases}$

6.6 Komplexe Zahlen der Länge 1 und Drehungen

Ist $a \in \mathbb{C}$, $|a| = 1$, so ist

$$f: \mathbb{C} \to \mathbb{C},\ z \mapsto az$$

eine Drehung um $\arg(a)$: $a = e^{i\alpha}$, $z = re^{i\varphi} \Rightarrow az = re^{i(\varphi+\alpha)}$.



Insbesondere ist

$$U(1) := \{z \in \mathbb{C} \mid |z| = 1\}$$

eine abelsche Gruppe und für jedes $n \in \mathbb{N}\setminus\{0\}$

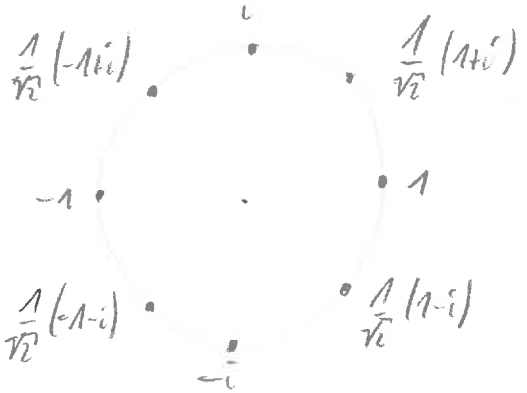
$$C_n := \{z \in \mathbb{C} \mid z^n = 1\} = \{e^{i\frac{k}{n}2\pi} \mid k = 0, \dots, n-1\}$$ n-te Einheitswurzeln

eine Untergruppe mit n Elementen, die isomorph zu $\mathbb{Z}/n$ ist:

$$\mathbb{Z}/n \to E_n,\ k \mapsto e^{i\frac{k}{n}2\pi}$$ ist ein Isom.

Bsp:

$n=8$:



6.7 Bem: Es gibt sehr viele andere Körper, z.B. für beliebiges $S \subset \mathbb{C}$ den kleinsten Unterkörper K von $\mathbb{C}$, der S enthält:

$$\mathbb{Q} \subset K := \bigcap_{\substack{L \subset \mathbb{R} \\ \text{Unterkörper}}} L \subset \mathbb{C}.$$

Ist $S = \{\alpha_1, \dots, \alpha_s\}$, so schreibt man $K = \mathbb{Q}(\alpha_1, \dots, \alpha_s)$.

Bsp: $\mathbb{Q}[\sqrt{8}] = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{2})$ (→ Übg. Blatt 4).

↗ Vorlesung Algebra.

§7. Der Begriff des Vektorraums

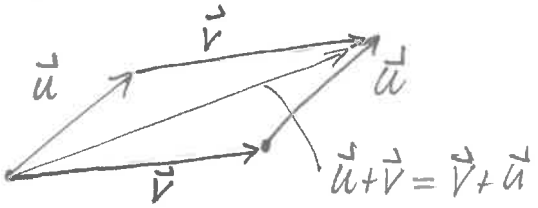
Vektorräume abstrahieren "Lineare Strukturen".

Beispiele / Motivation:

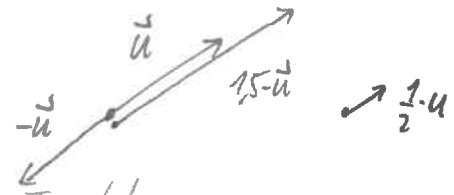
7.1 | Naive Vektorrechnung

"Ein (ebener) Vektor ist ein Pfeil in der Ebene, der beliebig parallel verschiebbar ist. Er ist eindeutig durch seine Länge, Richtung und Orientierung festgelegt." (d.h. Vektoren $\hat{=}$ {Pfeile} / Translationen)

Addition:



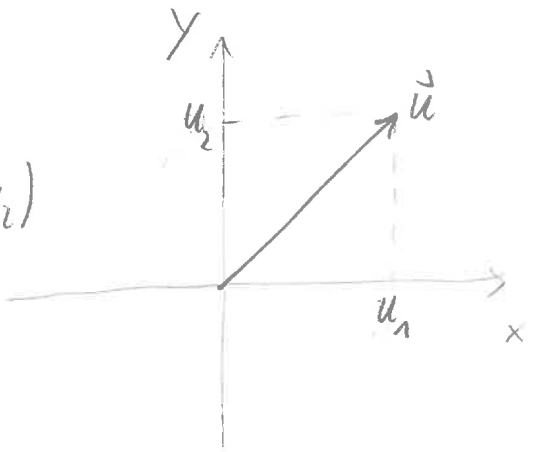
Streckung / Stauchung:



$\vec{u} \longmapsto \lambda \cdot \vec{u}$, $\lambda \in \mathbb{R}$

Alternativ: Vektor = Translation

7.2 | $\mathbb{R}^2$



Nach Wahl eines Koordinatensystems: $\vec{u} = (u_1, u_2)$

Addition: $(u_1, u_2) + (v_1, v_2) = (u_1+v_1, u_2+v_2)$

Streckung / Stauchung: $\lambda \cdot (u_1, u_2) = (\lambda u_1, \lambda u_2)$

7.3 K^n

Wir können ohne Mühe auch n statt 2 Einträge behandeln;

ferner können die Einträge aus einem beliebigen Körper K kommen.
"Skalare"

$$K^n := \underbrace{K \times \dots \times K}_{n\text{-mal}} = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in K\}.$$

Addition: $(\alpha_1, \dots, \alpha_n) + (\beta_1, \dots, \beta_n) := (\alpha_1 + \beta_1, \dots, \alpha_n + \beta_n)$, d.h. komponentenweise

Multiplikation mit Skalar: $\lambda \in K$, $\lambda \cdot (\alpha_1, \dots, \alpha_n) := (\lambda\alpha_1, \dots, \lambda\alpha_n)$.

7.4. → S.1.30

7.5 K-wertige Folgen ("K^∞", vgl. auch Analysis)

Eine K-wertige Folge ist eine Abbildung $a: \mathbb{N} \to K$.

Falls $a(n) = a_n$, so schreibt man auch (a_n).

$$(a_n) + (b_n) := (a_n + b_n), \quad \lambda \cdot (a_n) := (\lambda a_n).$$

7.6 K-wertige Abbildungen

Allgemeiner: Sei M eine beliebige Menge, so verhalten sich Abbildungen $M \to K$ wie Vektoren über K.

[" M = Indexmenge oder Einträge dieser Vektoren"]

$f, g \in \mathrm{Abb}(M, K)$, $\lambda \in K$, dann

$f + g: M \to K,\ x \mapsto f(x) + g(x)$

$\lambda f: M \to K,\ x \mapsto \lambda \cdot f(x)$

, d.h. "punktweise" definiert. (addiere bzw. multipliziere mit λ die Werte an den Elementen von M)

Die gleiche Definition funktioniert für Teilmengen ($\neq \emptyset$) $U \subset \mathrm{Abb}(M,K)$, sofern sie abgeschlossen unter diesen Operationen sind, d.h.

$\forall f,g \in U : f+g \in U$ (kurz: $U+U \subset U$)

$\forall f \in U \; \forall \lambda \in K : \lambda f \in U$. (kurz: $K \cdot U \subset U$)

z.B. $\mathcal{C}^0([a,b]) = \{f : [a,b] \to \mathbb{R} \text{ stetig}\}$

7.7 Lösungsräume linearer Differentialgleichungen (→ Analysis)

Für differenzierbare Funktionen $f,g : \mathbb{R} \to \mathbb{R}$ betrachte das System von Differentialgleichungen

$$\boxed{\begin{aligned} f' &= g \\ g' &= -f \end{aligned}} \quad (*)$$

Lösungen (f,g) von $(*)$ verhalten sich wie Vektoren über $\mathbb{R}$; denn

(f_1,g_1) und (f_2,g_2) lösen $(*)$ $\Rightarrow$ (f_1+f_2, g_1+g_2) löst $(*)$.

$\lambda \in \mathbb{R}$ und (f,g) löst $(*)$ $\Rightarrow$ $(\lambda f, \lambda g)$ löst $(*)$.

Bem: (f,g) löst $(*)$ $\Leftrightarrow$ $\exists \alpha,\beta \in \mathbb{R} : f(t) = \alpha \cdot \cos t + \beta \cdot \sin t$

$g(t) = -\alpha \sin t + \beta \cdot \cos t$.

Abstrakt gesehen ist dieses Beispiel also nichts anderes als 7.2 vermöge

$(\alpha,\beta) \longmapsto (\alpha \cos t + \beta \sin t, \; -\alpha \sin t + \beta \cos t)$

7.8 Körpererweiterungen

Ist L ein Körper und $K \subset L$ Unterkörper, so können wir die Elemente von L als Vektoren über K auffassen:

$u, v \in L \Rightarrow u+v \in L$

$\lambda \in K, u \in L \Rightarrow \lambda u \in L$. (gilt sogar für $\lambda \in L$, aber wir schränken uns bewusst auf $\lambda \in K$ ein)

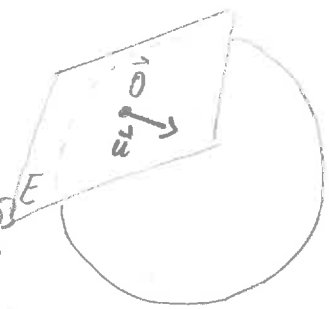
Bsp: a) $\mathbb{R} \subset \mathbb{C}$. Vgl. wieder 7.2 und 7.6: $\mathbb{R}^2 \to \mathbb{C}$ bij. $(\alpha, \beta) \mapsto \alpha + i\beta$

b) $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}^2 \to \mathbb{Q}[\sqrt{2}]$, $(\alpha, \beta) \mapsto \alpha + \beta\sqrt{2}$. bij.

c) $\mathbb{Q} \subset \mathbb{R}$: Eine riesige Menge von Vektoren!

7.4 Ebenen in $\mathbb{R}^3$

z.B. eine Tangential- (Schmiege-) ebene E an eine Kugel im $\mathbb{R}^3$.



Diese Vektoren lassen sich als $u = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{R}^3$ interpretieren, deren Komponenten α_i eine lineare Gleichung (Ebenengleichung) erfüllen:

$$\lambda_1\alpha_1 + \lambda_2\alpha_2 + \lambda_3\alpha_3 = 0 \quad , \quad \lambda_i \in \mathbb{R}, \ (\exists i : \lambda_i \neq 0)$$

Haben $u, v \in E \setminus \{0\}$ verschiedene Richtung, so liefert

$$(\alpha, \beta) \longrightarrow \alpha \cdot u + \beta \cdot v$$

eine Identifikation von $\mathbb{R}^2$ mit E (Wahl eines Koordinatensystems.)

7.9 (Abstrakte) Vektorräume

Ab jetzt: K sei ein fest gewählter Körper, falls nicht anders angegeben. ($\rightsquigarrow$ Skalare)

Def: Ein **K-Vektorraum** ist eine abelsche Gruppe $(V, +, 0_V)$ zusammen mit einer Abbildung (**Skalarmultiplikation**)

$$K \times V \longrightarrow V, \quad (\lambda, v) \longmapsto \lambda \cdot v,$$

so dass

(i) $\forall \lambda \in K \; \forall v, w \in V \quad \lambda \cdot (v+w) = \lambda \cdot v + \lambda \cdot w$

(ii) $\forall \lambda, \mu \in K \; \forall v \in V \quad (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$

(iii) $\forall \lambda, \mu \in K \; \forall v \in V \quad \lambda \cdot (\mu \cdot v) = (\lambda \mu) \cdot v$.

(iv) $\forall v \in V \quad 1 \cdot v = v$.

Elemente von V heißen **Vektoren**, Elemente von K **Skalare**.

Kurzschreibweisen: Der (K-) Vektorraum V (statt $(V, +, 0_V, K \times V \to V)$).

0 statt 0_V

λv statt $\lambda \cdot v$.

Beachte: Wir multiplizieren Skalare nur von links!

Bem: a) $\forall v: 0 \cdot v = 0_V$, $(-1) \cdot v = -v$:

$0_V + 0 \cdot v = 0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v$ / $0 \cdot v$ kürzen

$(-1) \cdot v + v = (-1) \cdot v + 1 \cdot v = (-1+1) \cdot v = 0 \cdot v = 0_V$.

(vgl. 4.8.1 und 4.8.2)

b) (ii)–(iv) $\Rightarrow \forall v \in V \setminus \{0\}$ ist $Kv < V$ stabil unter + und Sk.mult. und $K \longrightarrow Kv, \lambda \longmapsto \lambda v$ identifiziert diese mit + und $\cdot$ in K.

7.10 (i) – (iv) für K^n

$\lambda, \mu \in K, \; v = (\alpha_1, \ldots, \alpha_n), w = (\beta_1, \ldots, \beta_n) \in K^n$.

(i) $\lambda \cdot (v+w) = \lambda \cdot (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) = (\lambda(\alpha_1 + \beta_1), \ldots, \lambda(\alpha_n + \beta_n))$

$= (\lambda\alpha_1 + \lambda\beta_1, \ldots, \lambda\alpha_n + \lambda\beta_n) = (\lambda\alpha_1, \ldots, \lambda\alpha_n) + (\lambda\beta_1, \ldots, \lambda\beta_n) = \lambda v + \lambda w$.

(ii) $(\lambda+\mu)\cdot v = ((\lambda+\mu)\alpha_1, \dots, (\lambda+\mu)\alpha_n) = (\lambda\alpha_1+\mu\alpha_1, \dots, \lambda\alpha_n+\mu\alpha_n)$

$= (\lambda\alpha_1, \dots, \lambda\alpha_n) + (\mu\alpha_1, \dots, \mu\alpha_n) = \lambda v + \mu v.$

(iii) $\lambda\cdot(\mu\cdot v) = \lambda\cdot(\mu\alpha_1, \dots, \mu\alpha_n) = (\lambda\mu\alpha_1, \dots, \lambda\mu\alpha_n) = (\lambda\mu)\cdot(\alpha_1, \dots, \alpha_n).$

(iv) $1\cdot v = (1\alpha_1, \dots, 1\cdot\alpha_n) = (\alpha_1, \dots, \alpha_n) = v.$

7.1.1 Lineare Abbildungen

Dies sind die Homomorphismen zwischen Vektorräumen.

Def: Seien V, W K-Vektorräume. Eine Abbildung

$$\varphi: V \to W$$

heißt **(K-) linear**, falls

(i) φ ein Homom. abelsche Gruppen $(V,+) \to (W,+)$ ist.

(ii) $\forall \lambda \in K \ \forall v \in V: \varphi(\lambda\cdot v) = \lambda\cdot\varphi(v)$

Skalarmult. in V ; in W

Bem: a) (i) und (ii) sind äquivalent zu

$$\forall \lambda,\mu \in K \ \forall v,w \in V: \varphi(\lambda v + \mu w) = \lambda\varphi(v) + \mu\varphi(w).$$

[$\varphi(v+w) = \varphi(v)+\varphi(w)$: setze $\lambda=\mu=1$

$\varphi(\lambda\cdot v) = \lambda\cdot\varphi(v)$: setze $w=0_V$, $\mu=1$ $\quad \lambda\cdot v + 1\cdot 0_V = \lambda\cdot v + 0_V = \lambda v$

$\varphi(\lambda v) = \varphi(\lambda v + 1\cdot 0_V) = \lambda\cdot\varphi(v) + 1\cdot\varphi(0_V) = \lambda\cdot\varphi(v) + 1\cdot 0_W = \lambda\cdot\varphi(v)$]

(inj./surj.) (Bem 5.1, a) (Homom., Epim.)

b) Ist φ bijektiv, so redet man wie bei Homomorphismen von einem **Isomorphismus**.

Zwei (K-) Vektorräume heißen **isomorph**, falls es einen Isomorphismus $\varphi: V \to W$ gibt. Schreibweise: $V \simeq W$.

7.12 Bsp. V ein VR, dann

a) $\varphi: K = K^1 \to V$ linear $\iff \exists v \in V: \forall \alpha \in K \quad \varphi(\alpha) = \alpha \cdot v$

"$\Leftarrow$": $\varphi(\lambda\alpha + \mu\beta) = (\lambda\alpha + \mu\beta)\cdot v = \lambda\cdot(\alpha v) + \mu\cdot(\beta v) = \lambda\cdot\varphi(\alpha) + \mu\cdot\varphi(\beta)$.

"$\Rightarrow$": Setze $v := \varphi(1)$.

Dann gilt für $\alpha \in K$: $\varphi(\alpha) = \varphi(\alpha\cdot 1) = \alpha\cdot\varphi(1) = \alpha\cdot v$. //

b) $\varphi: K^n \to K = K^1$ linear $\iff \exists \alpha_1, \dots, \alpha_n \in K: \forall v = (v_1, \dots, v_n) \in K^n$
$\varphi(v) = \alpha_1 v_1 + \dots + \alpha_n \cdot v_n$.

"$\Leftarrow$": $\varphi(\lambda v + \mu w) = \varphi(\lambda v_1 + \mu w_1, \dots, \lambda v_n + \mu w_n)$

$= \alpha_1(\lambda v_1 + \mu w_n) + \dots + \alpha_n(\lambda v_n + \mu w_n)$

$= \lambda(\alpha_1 v_1 + \dots + \alpha_n w_n) + \mu(\alpha_1 w_1 + \dots + \alpha_n w_n)$

$= \lambda\varphi(v) + \mu\varphi(w)$.

"$\Rightarrow$": Setze $\alpha_i := \varphi(e_i)$, $e_i := (0, \dots, 0, 1, 0, \dots, 0) \in K^n$
(1 an i-te Stelle).

Dann gilt für $v = (v_1, \dots, v_n) \in K^n$: $v = v_1 e_1 + \dots + v_n e_n$, und daher

$\varphi(v) = v_1\varphi(e_1) + \dots + v_n\varphi(e_n) = \alpha_1 v_1 + \dots + \alpha_n v_n$.

c) $\varphi: K^2 \to K$, $(\lambda, \mu) \mapsto \lambda\mu$ ist nicht K-linear:

$1 = \varphi(1\cdot(1,1)) = \varphi((1,0) + (0,1)) \neq \varphi((1,0)) + \varphi((0,1)) = 0 + 0 = 0$.

d) $\varphi: K \to K$, $\alpha \mapsto \alpha^2$ ist nicht K-linear, außer $1+1=0$ in K:
(etwa $K = \mathbb{F}_2$).

$\varphi(1+1) = (1+1)^2 = 1 + 2\cdot 1 + 1$, aber $\varphi(1) + \varphi(1) = 1 + 1$.

5999 / 8700 (1.33 1/2)

Erläuterungen zu 7.12, a

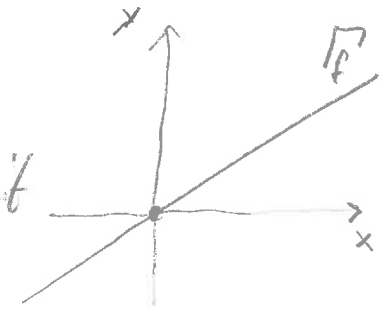
1. K ist als K-Vektorraum (↗ 7.8) gleich $K^1 = \underbrace{K \times \dots \times K}_{1\text{-mal}} = K$ (↗ 7.3).

2. Eine Abbildung

$$\varphi: K \to K$$

ist K-linear genau dann, wenn ein $\alpha \in K$ existiert mit

$$\varphi(x) = \alpha x. \qquad (v = \alpha \text{ in der Notation von Bsp a})$$



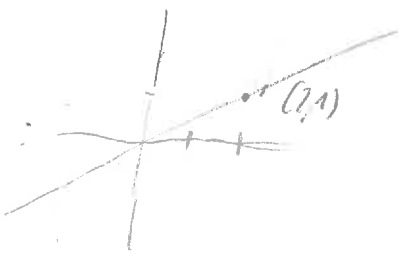
Vorsicht: In der Schule heißen Funktionen $f: \mathbb{R} \to \mathbb{R}$, $f(x) = mx + a$ linear; präziser spricht man für $a \neq 0$ aber von affinen Funktionen.

Eine lineare Abbildung $\varphi: V \to W$ erfüllt $\varphi(0_V) = 0_W$!

3. $V = \mathbb{R}^2$, $v = (2,1)$

$$\varphi: \mathbb{R} \to \mathbb{R}^2, \quad \alpha \longmapsto (2\alpha, \alpha)$$

$\mathrm{im}(\varphi)$:



---

zu 7.12, b

$K = \mathbb{R}$, $n = 2$, $\alpha_1 = 1$, $\alpha_2 = 2$:

$$\varphi: \mathbb{R}^2 \to \mathbb{R}, \quad \varphi(v_1, v_2) = v_1 + 2v_2$$

7.13 | Bspe aus der Analysis

a) $V = \{ f : \mathbb{R} \to \mathbb{R} \text{ differenzierbar} \}$

$W = \mathrm{Abb}(\mathbb{R}, \mathbb{R})$.

Die folgenden Abbildungen sind linear:

$D : V \to W, \quad f \mapsto f'$

$ev_0 : W \to \mathbb{R}, \quad f \mapsto f(0)$ Auswertung in $x=0$ (engl.: evaluation)

$\varphi : V \to \mathbb{R}^2, \quad f \mapsto (f(0), f'(0))$

$\int_0^1 : V \to \mathbb{R}, \quad f \mapsto \int_0^1 f(t)\,dt$.

---

b) $V = \{ (a_n)_{n \in \mathbb{N}} \mid a_n \in \mathbb{R}, (a_n) \text{ konvergiert gegen eine reelle Zahl} \} \subset \mathrm{Abb}(\mathbb{N}, \mathbb{R})$ — konvergente reelle Folgen ist ein $\mathbb{R}$-VR. (vgl. 7.5)

$\lim : V \to \mathbb{R}, \quad (a_n) \mapsto \lim_{n \to \infty} a_n$ ist linear.

7.14 | Unterräume (= Unterobjekte in Vektorräumen)

Diese verallgemeinern Geraden und Ebenen im $\mathbb{R}^3$, die den Nullpkt enthalten.

Def: Sei V ein K-Vektorraum. Ein Unterraum (Untervektorraum) von V ist eine Teilmenge $U \subset V$ mit den Eigenschaften:

(i) $0 \in U$

(ii) $\forall v, w \in U : v + w \in U$

(iii) $\forall v \in U \; \forall \lambda \in K : \lambda v \in U$

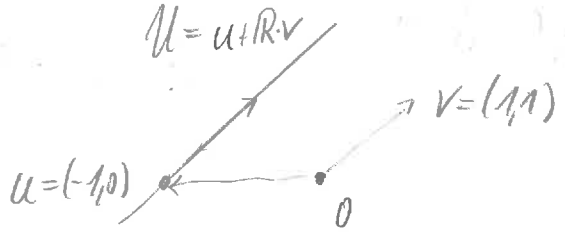
} d.h. $U \subset (V, +)$ Ugrp.

Bem: a) $(U, +, \cdot)$ ist dann auch ein abstrakter Vektorraum.

b) (i)–(iii) $\Leftrightarrow$ $U \neq \emptyset$ und $\forall \lambda,\mu \in K \; \forall v,w \in U : \lambda v + \mu w \in U$ (vgl. Üb. 6.3)

Diskussion von (i) — (iii) durch Nicht-Beispiele, $V = \mathbb{R}^2$

(i)

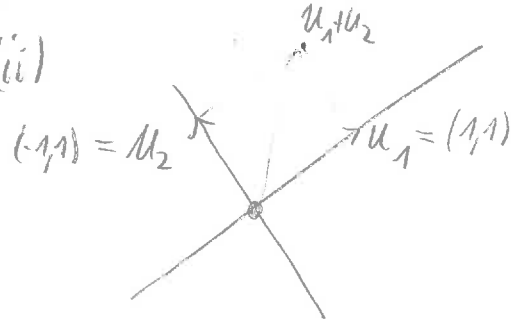


$U = \{u + \lambda v \mid \lambda \in \mathbb{R}\}$

ist kein UR $(0 \notin U)$.

(später: affiner Unterraum)

(ii)



$u_1 \neq 0,\; u_2 \in \mathbb{R}^2 \setminus \mathbb{R}\cdot u_1$

$U := \mathbb{R}u_1 \cup \mathbb{R}u_2$ ist kein UR $\left(\begin{smallmatrix}\exists u_1, u_2 \\ u_1 + u_2 \notin U\end{smallmatrix}\right)$

(iii) $U := \mathbb{Z}^2$ ist Untergruppe von $(\mathbb{R}^2, +)$, aber kein UR:

$(1,1) \in U$, aber $\frac{1}{2}(1,1) = \left(\frac{1}{2}, \frac{1}{2}\right) \notin U$.

1.15 Beispiele

a) $\{0\} \subset V$ und $V \subset V$ sind (triviale) Unterräume

b) Unterräume von $\mathbb{R}^3$: $\{0\}$

Geraden durch 0: $U = \mathbb{R}\cdot v$, $v \neq 0$.

Ebenen durch 0: $U = \mathbb{R}\cdot v + \mathbb{R}\cdot w$, $v \neq 0$, $w \in \mathbb{R}^2 \setminus \mathbb{R}\cdot v$.

$\mathbb{R}^3$.

Später: Dies sind alle!

c) $\{(a_n)$ konvergente Folge in $\mathbb{R}\} \subset \mathrm{Abb}(\mathbb{N}, \mathbb{R}) = \{$alle Folgen in $\mathbb{R}\}$

ist ein UR.

7.16 | Summen und Durchschnitte

Satz Seien V ein Vektorraum und $U_1, U_2 \subset V$ Unterräume.

a) Die **Summe**

$$U_1 + U_2 = \{ u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2 \}$$

ist der kleinste Unterraum von V, der $U_1 \cup U_2$ enthält:

$$\forall U \subset V \text{ Unterraum}, U_1 \cup U_2 \subset U : U_1 + U_2 \subset U. \quad (*)$$

b) Der **Durchschnitt** $U_1 \cap U_2$ ist der größte Unterraum, der sowohl in U_1 enthalten ist, als auch in U_2:

$$\forall U \subset V \text{ Unterraum}, U \subset U_1, U \subset U_2 \Rightarrow U \subset U_1 \cap U_2. \quad (*)$$

Bew: Dass $U_1 + U_2$ und $U_1 \cap U_2$ Unterräume sind, folgt durch einfaches Überprüfen von (i) – (iii) in Def. 7.14.

Etwa (ii) in (a): $v = u_1 + u_2 \in U_1 + U_2$, $w = u_1' + u_2' \in U_1 + U_2$

$$\Rightarrow v + w = (u_1 + u_1') + (u_2 + u_2') \in U_1 \cup U_2.$$

Es bleiben die Eigenschaften (*) zu zeigen.

a) Sei $U \subset V$ UR und $U_1 \cup U_2 \subset U$.

$u \in U_1 + U_2 \Rightarrow \exists u_1 \in U_1, u_2 \in U_2 : u = u_1 + u_2$

Wegen $U_1 \subset U, U_2 \subset U$ gilt $u_1, u_2 \in U$.

$\overset{U \text{ UR}}{\Rightarrow} u_1 + u_2 \in U. \Rightarrow u \in U.$

b) Diese Implikation folgt rein mengentheoretisch.

□//

Vorsicht: Der Durchschnitt zweier Unterräume ist ein Unterraum, ihre Vereinigung im allgemeinen nicht (↳ Diskussion von (ii) in 7.14). Jedoch

7.18 Historisches

William R. Hamilton 1843: Quaternionen

Hermann Graßmann 1844: "Die lineale Ausdehnungslehre..."

Hermann Weyl 1917: "Raum-Zeit-Materie" (axiomatischer Vektorbegriff)

7.17 Kerne und Bilder

Satz: Sind V, W K-Vektorräume und $\varphi: V \to W$ linear, so sind

Kern (vgl. S. 4) und Bild von $\varphi: (V,+) \to (W,+)$,

$$\ker(\varphi) := \{v \in V \mid \varphi(v) = 0_W\},$$
$$\operatorname{im}(\varphi) := \varphi(V) = \{\varphi(v) \mid v \in V\},$$

Unterräume von V bzw. W.

Bew: Wir überprüfen Satz 7.14, b:

$\ker(\varphi) \neq \emptyset$ $(0_V \in \ker \varphi)$.

$$\lambda, \mu \in K,\ v, w \in \ker(\varphi) \Rightarrow \varphi(\lambda v + \mu w) = \lambda\varphi(v) + \mu\varphi(w) = \lambda \cdot 0_W + \mu \cdot 0_W = 0_W$$
$$\Rightarrow \lambda v + \mu w \in \ker(\varphi)$$

$\operatorname{im}(\varphi) \neq \emptyset$ $(0_W = \varphi(0_V) \in \operatorname{im}(\varphi))$

$$\lambda, \mu \in K,\ v, w \in \operatorname{im}(\varphi) \Rightarrow \exists v', w' \in V : v = \varphi(v'),\ w = \varphi(w') \Rightarrow \lambda v + \mu w = \varphi(\lambda v' + \mu w') \in \operatorname{im}(\varphi).$$

□

...bildung geboren, wurde 1831 Lehrer in Stettin (dem heutigen Szczecin), wo er bis zu seinem Tode blieb. Aber seine Interessen waren äußerst vielseitig: Graßmann arbeitete zeitweilig in der Redaktion der „Norddeutschen Zeitung", sammelte pommersche Volkslieder und war Vorsitzender des „Pommerschen Hauptvereins für die Evangelisierung Chinas". Bis heute kann man in zwei völlig unterschiedlichen Wissenschaftsgebieten seine Nachwirkung feststellen: In der Sprachwissenschaft – und in der Mathematik.

Graßmanns sprachwissenschaftliche Studien kulminierten in der Übersetzung der *Rigveda*, einer Sammlung altindischer religiöser Texte und Lieder, und der Herausgabe eines dazugehörigen Wörterbuches; für diese Leistung wurde ihm 1876 die Ehrendoktorwürde der Universität Tübingen verliehen.

Die für uns wichtigste Leistung Graßmanns besteht aber in der Mathematik. In seiner Ausdehnungslehre hat er bereits den Begriff eines n-dimensionalen Vektorraums, und zwar den eines „allgemeinen" Vektorraums (also nicht nur des K^n) ausdrücklich vorgestellt. Er schreibt:

> Es geht darum, die sinnlichen Anschauungen der Geometrie zu allgemeinen, logischen Begriffen zu erweitern und zu vergeistigen ... Ich sage, eine Größe a sei aus den Größen b, c, ... durch die Zahlen β, γ, ... abgeleitet, wenn $a = \beta b + \gamma c + \ldots$ Dabei seien β, γ, ... reelle Zahlen.
>
> Die Größen a, b, c, ... stehen zueinander in einer Zahlbeziehung, wenn irgend eine sich aus den anderen numerisch berechnen lässt ... Einheit nenne ich jede Größe, welche dazu dienen soll, um aus ihr eine Reihe von Größen abzuleiten. Ein System von Einheiten nenne ich jeden Verein von Größen, welche in keiner Zahlbeziehung zueinander stehen und welche dazu dienen sollen, um aus ihnen durch beliebige Zahlen andere Größen abzuleiten. Die algebraischen Größen heißen auch extensive Größen.
>
> Für extensive Größen gelten die Fundamentalformeln:
>
> $$a + b = b + a$$
> $$a + (b + c) = (a + b) + c$$
> $$a + b - b = a;$$
>
> a, b, c sind Größen, α, β reelle Zahlen:
>
> $$\alpha a = a\alpha$$
> $$\alpha(\beta a) = (\alpha\beta)a$$
> $$\alpha(a + b) = \alpha a + \alpha b$$
> $$a(\alpha + \beta) = a\alpha + a\beta$$
> $$1a = a.$$
>
> Die Gesamtheit der Größen, welche aus einer Reihe von Größen $a_1, a_2, \ldots, a_n$ numerisch ableitbar sind, nenne ich das aus jenen Größen ableitbare Gebiet n-ter Stufe, wenn jene Größen von erster Stufe sind und sich das Gebiet nicht aus weniger als n solchen Größen ableiten läßt. Jedes Gebiet n-ter Stufe kann aus n (ihm angehörenden) Größen erster Stufe, die in keiner Zahlbeziehung zueinander stehen, abgeleitet werden, und zwar aus beliebigen n solchen Größen des Gebiets.

...Materialien...

1. Vektoren

Je zwei Vektoren a und b bestimmen eindeutig einen Vektor a+b als ihre „Summe"; eine
ein Vektor a bestimmen eindeutig einen Vektor λa, das „λ-fache von a" (Multiplikation). D
onen genügen den folgenden Gesetzen:

a) Addition.

i. $a + b = b + a$ (kommutatives Gesetz).

ii. $(a + b) + c = a + (b + c)$ (assoziatives Gesetz).

iii. Sind a und c irgend zwei Vektoren, so gibt es einen und nur einen Vektor x, fü
Gleichung $a + x = c$ gilt. Er heißt die Differenz c–a von c und a (Möglichkeit der Subt

b) Multiplikation

i. $(\lambda + \mu)a = (\lambda a) + (\mu a)$ (erstes distributives Gesetz).

ii. $\lambda(\mu a) = (\lambda\mu)a$ (assoziatives Gesetz).

iii. $1a = a$.

iv. $\lambda(a + b) = (\lambda a) + (\lambda b)$ (zweites distributives Gesetz).

Dimensionsaxiom: Es gibt n linear unabhängige Vektoren, aber je n+1 sind voneinander lin

Spätestens seit B. L. van der Waerdens Buch *Moderne Algebra* 1936 hat sich des Vektorraums über einem beliebigen Körper eingebürgert (van der Waerde sogar Vektorräume über Schiefkörpern!) und ist heute aus keiner Mathemati mehr wegzudenken.

Weitere Informationen zur Geschichte der Linearen Algebra finden Sie in [und [Scho], Kapitel 13. das Werk Graßmanns wird ausführlich in [Zad] vorgeste

Richtig oder falsch?

1 Thema: Definition eines Vektorraums

☐ Man kann je zwei Vektoren eines Vektorraums addieren.

☐ Man kann einen Vektor v durch einen Vektor w dividieren, falls $w \neq o$

☐ Jeder Vektorraum hat ein eindeutiges Nullelement.

☐ Jeder Vektorraum hat ein eindeutiges Einselement.

☐ Wenn V ein K-Vektorraum ist, dann ist $\{v+w \mid v \in V, w \in V\} = V$.

☐ Wenn V ein K-Vektorraum ist, dann ist $\{v+w \mid v \in V, w \in V\} = V \times V$.

☐ Für alle u, v, w eines Vektorraums V gilt $u \cdot (v \cdot w) = (u \cdot v) \cdot w$.

§.8 Basis und Dimension

Um in abstrakten Vektorräumen arbeiten zu können, brauchen wir ein (lineares) Koordinatensystem. Dieses erhält man durch eine "Basis":

In $\mathbb{R}^n$: $(\lambda_1, \dots, \lambda_n) = \lambda_1 e_1 + \dots + \lambda_n e_n$

In V: Finde $v_1, \dots, v_n$, so dass sich jedes $v \in V$ eindeutig schreiben lässt als $\lambda_1 v_1 + \dots + \lambda_n v_n$, $\lambda_i \in K$.

Bsp $\mathbb{R}^2$ ✓?

8.1 | Linearkombinationen

Def: Sei V ein K-Vektorraum. Ein $v \in V$ heißt Linearkombination von $v_1, \dots, v_n \in V$, falls $\lambda_1, \dots, \lambda_n \in K$ existieren mit

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

Die Menge aller Linearkombinationen von $v_1, \dots, v_n$,

$$L(v_1, \dots, v_n) := \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in K \right\}$$

heißt lineare Hülle (Erzeugnis) der v_i.

Ist $U \subset V$ ein Unterraum, so erzeugen $v_1, \dots, v_n$ diesen Unterraum falls $U = L(v_1, \dots, v_n)$. (Auch: $v_1, \dots, v_n$ spannen U auf).

Bem: Es ist auch sinnvoll, das Erzeugnis einer (eventuell unendlichen)

Teilmenge $S \subset V$ zu nehmen. Allerdings können wir nur endliche Linearkombinationen zulassen (was wäre $\sum_{n \in \mathbb{N}} (1,n)$?), d.h.

$$L(S) := \{ v \in V \mid \exists n \in \mathbb{N}\ \exists v_1, \dots, v_n \in V\ \exists \lambda_1, \dots, \lambda_n \in K : v = \sum_{i=1}^{n} \lambda_i v_i \}.$$

---

§2 Beispiele

a) $e_1, \dots, e_n$ erzeugen K^n

b) $(2,1), (1,3)$ erzeugen $\mathbb{R}^2$, ebenso $(2,1), (1,3), (1,0)$.

c) $(1,0,1), (0,1,-2)$ spannen die Ebene

$$\{(\lambda, \mu, \lambda - 2\mu) \mid \lambda, \mu \in \mathbb{R}\} \subset \mathbb{R}^3 \text{ auf.}$$

d) $S = \{e_i \mid i \in \mathbb{N}\}$ erzeugen nicht $\mathrm{Abb}(\mathbb{N}, K) = \{(a_n)\}$, da für $(a_n) = \lambda_{i_1} e_{i_1} + \dots + \lambda_{i_n} e_{i_n}$ nur endlich viele $a_n \neq 0$ sind.

So gilt etwa: $(a_n) = (1,0,1,0,\dots) \notin L(S)$.

---

§3 Lineare Unabhängigkeit

Um die Eindeutigkeit der Darstellung $v = \lambda_1 v_1 + \dots + \lambda_n v_n$ zu erreichen, muss man die Menge $\{v_1, \dots, v_n\}$ minimal wählen:

Bsp: $v_1 = (2,1)$, $v_2 = (2,3)$, $v_3 = (1,0)$

$v = (1,1)$

Es gilt: $v = v_1 - v_3 = \frac{1}{4} v_1 + \frac{1}{4} v_2$.

Grund für die Nichteindeutigkeit ist die Relation

$$4v_1 - 4v_3 = v_1 + v_2$$

oder $3v_1 - v_2 - 4v_3 = 0$.

Def: $v_1, \dots, v_n \in V$ heißen <u>linear unabhängig</u>, falls

$$\forall \lambda_1, \dots, \lambda_n \in K: \lambda_1 v_1 + \dots + \lambda_n v_n = 0 \Rightarrow \lambda_1 = \dots = \lambda_n = 0,$$

Andernfalls heißen $v_1, \dots, v_n$ <u>linear abhängig</u>. In diesem Fall gilt:

$$\exists \lambda_1, \dots, \lambda_n \in K \; \exists i: \lambda_i \neq 0 \text{ und } \lambda_1 v_1 + \dots + \lambda_n v_n = 0.$$

Bem: Wieder kann man lineare Unabhängigkeit auch für Mengen $S \subset V$ definieren:

$$\forall n \in \mathbb{N} \; \forall v_1, \dots, v_n \in V \; \forall \lambda_1, \dots, \lambda_n \in K \; \left(\forall i \neq j \; v_i \neq v_j \Rightarrow \lambda_1 = \dots = \lambda_n = 0 \right).$$

8.4 Beispiele

a) $e_1, \dots, e_n \in K^n$ sind linear unabhängig:

Seien $\lambda_1, \dots, \lambda_n \in K$ und $\sum \lambda_i e_i = 0$.

Dann gilt $(\lambda_1, \dots, \lambda_n) = \sum \lambda_i e_i = 0$.

$\Rightarrow \lambda_1 = 0, \dots, \lambda_n = 0$.

b) $v_1 = (2,1)$, $v_2 = (2,3)$ sind linear unabhängig:

$\lambda_1 v_1 + \lambda_2 v_2 = 0$

$\Rightarrow (2\lambda_1 + 2\lambda_2, \lambda_1 + 3\lambda_2) = 0$

$\Rightarrow$ (I) $2\lambda_1 + 2\lambda_2 = 0$ (II) $\lambda_1 + 3\lambda_2 = 0$

$\Rightarrow$ (I) -2(II): $-\lambda_2 = 0$

$\Rightarrow \lambda_1 = \lambda_2 = 0$.

Beobachtung: Lineare Unabhängigkeit im K^n - bedeutet, dass ein homogenes lineares Gleichungssystem (in den Variablen $\lambda_1, \dots, \lambda_n$) nur die triviale Lösung $\lambda_1 = \dots = \lambda_n = 0$ hat.

2.5 Elimination von Erzeugern

Sind $v_1, \dots, v_n$ linear abhängig, so lässt sich einer der v_i als Linearkombination der übrigen v_j ausdrücken:

Satz: Sei V ein K-Vektorraum und $v_1, \dots, v_n \in V$ linear abhängig. Dann existiert ein $i \in \{1, \dots, n\}$ und $\mu_j \in K$, $j \in \{1, \dots, n\} \setminus \{i\}$ mit

$$v_i = \sum_{j \neq i} \mu_j v_j .$$

Bew: $\exists \lambda_1, \dots, \lambda_n \in K$ mit $\sum \lambda_j v_j = 0$ und $\exists i : \lambda_i \neq 0$.

$\Rightarrow -\lambda_i v_i = \sum_{j \neq i} \lambda_j v_j$

$\overset{\lambda_i \neq 0!}{\Rightarrow} v_i = \sum \left(-\frac{\lambda_j}{\lambda_i}\right) v_j$. Setze $\mu_j := \frac{-\lambda_j}{\lambda_i}$. □

Bem: Vorsicht, man kann i.a. nicht $i=1$ wählen.

Bsp: $v_1=(2,1)$, $v_2=(2,2)$, $v_3=(3,3)$

Es gilt $v_1 \notin L(v_2,v_3)$, aber

$v_2 = 0\cdot v_1 + \frac{2}{3} v_2$ und $v_3 = 0\cdot v_1 + \frac{3}{2} v_2$.

[$i=1$: nicht OK

$i=2,3$: OK.]

Folgerung: a) $v_1 \in V$ ist linear unabhängig $\Leftrightarrow v_1 \neq 0$.

b) $v_1, v_2 \in V$ sind linear unabhängig $\Leftrightarrow v_1 \neq 0$, $v_2 \notin L(v_1)$ (d.h. $v_2 \in V \setminus K\cdot v_1$).

$\Leftrightarrow v_2 \neq 0$, $v_1 \notin L(v_2)$

8.6 Basen

Def: Sei V ein K-Vektorraum. Eine Basis von V ist ein Tupel $(v_1,\dots,v_n)$, $v_i \in V$, für ein $n \in \mathbb{N}$ mit

(i) $v_1,\dots,v_n$ erzeugen V

(ii) $v_1,\dots,v_n$ sind linear unabhängig.

Merksatz: Eine Basis ist ein linear unabhängiges Erzeugendensystem.

Notationsmissbrauch: "Sei $v_1,\dots,v_n$ eine Basis".

Bem: a) Man kann eine Basis auch als linear unabhängige Menge $S \subset V$ definieren mit $V = L(S)$. Dies ist (z.B.) erforderlich, wenn es keine Basis endlicher Länge n gibt, etwa für $\mathrm{Abb}(\mathbb{N},K)$.

Unsere Definition ist leichter zu handhaben, wenn wir lineare Abbildungen durch Matrizen repräsentieren.

Beachte: $v_1,v_2,v_3,\dots,v_n$ und $v_2,v_1,v_3,\dots,v_n$ sind verschiedene Basen.

b) In der Quantenmechanik benutzt man einen anderen Basisbegriff, der auch unendliche (konvergierende) Linearkombinationen zulässt. Vgl. Funktionalanalysis.

Bsp: a) $e_1, \dots, e_n$ ist eine Basis für K^n. Man nennt sie die kanonische Basis.

b) $(1,2), (2,3)$ ist eine Basis für K^2.

8.7 Eindeutige Darstellbarkeit (Satz vom Koordinatensystem).

Satz: Sei V ein K-Vektorraum und $v_1, \dots, v_n \in V$ eine Basis. Dann gibt es für alle $v \in V$ eindeutige $\lambda_1, \dots, \lambda_n \in K$ mit

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

Bem: $(\lambda_1, \dots, \lambda_n)$ kann man als "Koordinate" von v bzgl. des durch $v_1, \dots, v_n$ definierten linearen Koordinatensystem ansehen.

Bew: Da $V = L(v_1, \dots, v_n)$ existieren $\lambda_1, \dots, \lambda_n \in K$ mit $v = \lambda_1 v_1 + \dots + \lambda_n v_n$.

Eindeutigkeit: Seien $\lambda_1, \dots, \lambda_n \in K$ und $\lambda_1', \dots, \lambda_n' \in K$ mit

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n = \lambda_1' v_1 + \dots + \lambda_n' v_n.$$

$$\Rightarrow (\lambda_1' - \lambda_1) v_1 + \dots + (\lambda_n' - \lambda_n) v_n = 0$$

$\Rightarrow$ ($v_1, \dots, v_n$ linear unabh.) $\lambda_1' - \lambda_1 = \dots = \lambda_n' - \lambda_n = 0 \Rightarrow \forall i: \lambda_i' = \lambda_i$.

□

8.8 Interpretation durch $\varphi: K^n \to V$.

Gegeben $v_1, \dots, v_n \in V$, so erhalten wir die lineare Abb.

$$\varphi: K^n \longrightarrow V, \quad (\lambda_1, \dots, \lambda_n) \longmapsto \sum \lambda_i v_i$$

mit der charakterisierenden (d.h. sie eindeutig festlegenden) Eigenschaft

$$\varphi(e_i) = v_i \quad , i = 1, \dots, n.$$

Jede lineare Abb. $\varphi: K^n \to V$ erhält man auf diese Weise; denn

$$\varphi(\lambda_1, \dots, \lambda_n) = \varphi\Big(\sum_{i=1}^{n} \lambda_i e_i\Big) = \sum_{i=1}^{n} \lambda_i \cdot \varphi(e_i) = \sum_{i=1}^{n} \lambda_i v_i \quad \text{mit } v_i = \varphi(e_i).$$

Satz: a) $v_1, \dots, v_n \in V$ erzeugen V $\iff$ φ ist surjektiv

b) $v_1, \dots, v_n \in V$ sind linear unabhängig $\iff$ φ ist injektiv

c) $v_1, \dots, v_n \in V$ sind eine Basis $\iff$ φ ist bijektiv.

Bew: (c) folgt aus (a) und (b).

(a) $L(v_1, \dots, v_n) = \operatorname{im}(\varphi)$.

(b) $\sum \lambda_i v_i = 0 \iff (\lambda_1, \dots, \lambda_n) \in \ker(\varphi) = \{u = (\mu_1, \dots, \mu_n) \in K^n \mid \varphi(u) = 0\}$

(= der Kern der Gruppenhom $(K^n, +) \to (V, +)$).

Demnach: $v_1, \dots, v_n$ lin. unabh. $\iff \ker(\varphi) = \{0\}$

$\overset{\text{Satz 5.5}}{\iff}$ φ injektiv.

□

8.9 Zum weiteren Vorgehen:

Ein Vektorraum V heißt endlich erzeugt, falls er durch endlich viele Elemente aufgespannt werden kann (d.h. $\exists$ Epimorphismus $K^n \to V$).
Für solches V wollen wir zeigen,

1. V besitzt eine Basis $v_1, \dots, v_n$.
2. Je zwei Basen haben die gleiche Länge n.
   (wir definieren dann $\dim V := n$ Dimension von V).

(1) kann man leicht beweisen, indem man aus Erzeugern $v_1, \dots, v_n$ so lange Elemente entfernt (mit 8.5), bis sie linear unabhängig werden ("Basisauswahlsatz").

(2) folgt dann dadurch, dass man linear unabhängige $w_1, \dots, w_m$ stets mit $n-m \geq 0$ Elementen von $v_1, \dots, v_n$ zu einer Basis ergänzen kann ("Steinitzscher Austauschsatz").

Wir werden etwas ökonomischer vorgehen und (1) und (2) als leichte Folgerungen aus dem etwas technischeren Resultat 8.10 und 8.11 herleiten.

8.10 Satz (Basisergänzungssatz)

Seien V ein K-Vektorraum und $w_1, \dots, w_k \in V$ Erzeuger von V:

$$V = L(w_1, \dots, w_k).$$

Sind dann $v_1, \dots, v_r \in V$ linear unabhängig, so existieren $s \geq 0$ und $j(1), \dots, j(s) \in \{1, \dots, k\}$ mit der Eigenschaft

$$\boxed{v_1, \dots, v_r, w_{j(1)}, \dots, w_{j(s)} \text{ ist eine Basis von } V.}$$

[d.h. "jedes linear unabhängige System von Vektoren kann durch Elemente einer erzeugenden Menge zu einer Basis ergänzt werden."]

Bsp: $V = \mathbb{R}^3$, $w_i = e_i$, $i = 1,2,3$ $\quad (k=3)$

$v_1 = (1,0,1)$, $v_2 = (1,0,0)$ $\quad (r=2)$

v_1, v_2, w_1 ist keine Basis: $\quad v_2 - w_1 = 0$

v_1, v_2, w_3 " keine " : $\quad v_1 - v_2 - w_3 = 0$

v_1, v_2, w_2 ist eine Basis: $\quad s=1,\ j(1)=2.$

Im Bew. benutzen wir:

Lemma (=Hilfssatz): Seien $v_1, \dots, v_r \in V$ linear unabhängig und $w \in V$. Dann gilt

$v_1, \dots, v_r, w$ linear abhängig $\Leftrightarrow w \in L(v_1, \dots, v_r)$. [vgl. 8.5!]

Bew: "$\Rightarrow$": $\exists\, \lambda_1, \dots, \lambda_r, \lambda \in K : \sum_{i=1}^{r} \lambda_i v_i + \lambda w = 0$ und $(\lambda \neq 0$ oder $\exists i : \lambda_i \neq 0)$.

Angenommen $\lambda = 0$. Dann gilt $\sum_{i=1}^{r} \lambda_i v_i = 0 \overset{v_1,\dots,v_r \text{ lin. unabh.}}{\Longrightarrow} \lambda_1 = \dots = \lambda_r = 0$ ↯.

Also $\lambda \neq 0$ und $w = \sum_{i=1}^{r} \left(-\frac{\lambda_i}{\lambda}\right) v_i \in L(v_1, \dots, v_r)$.

"$\Leftarrow$": $w \in L(v_1, \dots, v_r)$

$\Rightarrow \exists \lambda_1, \dots, \lambda_r : w = \sum_{i=1}^{r} \lambda_i v_i$, d.h. $\sum_{i=1}^{r} \lambda_i v_i + (-1) \cdot w = 0$

$\Rightarrow v_1, \dots, v_r, w$ sind linear abhängig. □

Tafel 1

Bew. des Satzes: Idee: Füge sukzessive w_i hinzu, sofern wir dadurch den aufgespannten Unterraum vergrößern.

1. Betrachte

$$U_i := L(v_1, \dots, v_r, w_1, \dots, w_i), \quad i = 0, \dots, k \qquad \left(\begin{array}{l} i=0 \text{ liefert:} \\ L(v_1, \dots, v_r) \end{array}\right)$$

Es gilt

$$L(v_1, \dots, v_r) = U_0 \subset U_1 \subset U_2 \subset \dots \subset U_k = L(v_1, \dots, v_r, w_1, \dots, w_k) = V.$$

Definiere $j(1) < \dots < j(s)$ als die "Sprungstellen" der Folge der U_i:

$$\{j(1), \dots, j(s)\} = \{i \in 1, \dots, k \mid U_{i-1} \neq U_i\}.$$

Setze ferner $j(0) := 0$.

2. Beh: Für $i \in \{1, \dots, k\}$ sei $\nu \in \{0, \dots, s-1\}$ so, dass

$$j(\nu) \leq i < j(\nu+1).$$

Dann gilt

$$U_i = L(v_1, \dots, v_r, w_{j(1)}, \dots, w_{j(\nu)}) \qquad \left(\begin{array}{l} \nu=0 \text{ bedeutet wieder:} \\ L(v_1, \dots, v_r) \end{array}\right)$$

Bew: Induktion nach i.

$i=0$: $U_0 = L(v_1, \dots, v_r)$ ✓

$i \to i+1$: Sei ν so, dass $j(\nu) \leq i < j(\nu+1)$.

↕ 2

↕ 1

Fall 1: $i+1 < j(\nu+1)$

Dann $U_{i+1} = U_i \overset{\text{Ind.Vor.}}{=} L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu)})$.

Fall 2: $i+1 = j(\nu+1)$

Dann $U_{i+1} = L(v_1, \dots, v_\nu, w_1, \dots, w_{i+1}) = L(v_1, \dots, v_\nu, w_1, \dots, w_i) + K \cdot w_{i+1}$

$\overset{\text{Ind.Vor.}}{=} L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu)}) + K \cdot w_{j(\nu+1)}$

$= L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu+1)})$.

↕ 4

3. Beh: $v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu)}$ sind linear unabhängig, $\nu = 0, \dots, s$.

Bew.: Induktion nach ν.

$\nu = 0$: $v_1, \dots, v_\nu$ sind lin. unabh.

$\nu \to \nu+1$: $v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu)}$ sind lin. unabh. nach Induktion.

$L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu)}) = U_{j(\nu)} \neq U_{j(\nu+1)} = L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu+1)})$

Lemma $\Rightarrow$ $v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(\nu+1)}$ sind lin. unabh.

↕ 5

4. Demnach ist $v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(s)}$ eine Basis:

$V = U_k = L(v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(s)})$ nach 2.

$v_1, \dots, v_\nu, w_{j(1)}, \dots, w_{j(s)}$ lin. unabh. nach 3.

□

8.11 Zusatz zu Satz 8.10: Es gilt $r \leq k$.

Bew: o.E. sei die Numerierung der v_i so, dass

$v_{n+1}, \dots, v_r \in \{w_1, \dots, w_k\}$, $v_1, \dots, v_n \notin \{w_1, \dots, w_k\}$. $(n \in \{0, \dots, k\})$.

und $w_1, \dots, w_k$ seien paarweise verschieden.

Bew. durch Induktion nach $n = \#\{i \mid v_i \notin \{w_1, \dots, w_k\}\}$.

$n=0$: $\{v_1, \dots, v_r\} \subset \{w_1, \dots, w_k\} \Rightarrow r \leq k$.

$n \to n+1$: $v_1, \dots, v_{n+1} \notin \{w_1, \dots, w_k\}$, $v_{n+2}, \dots, v_r \in \{w_1, \dots, w_k\}$.

Wende Satz 8.10 an auf

$v_1, \dots, v_n, v_{n+2}, \dots, v_r$ (v_{n+1} fortlassen!) und $w_1, \dots, w_k$.

$\Rightarrow \exists j(1), \dots, j(s)$: $v_1, \dots, v_n, v_{n+2}, \dots, v_r, w_{j(1)}, \dots, w_{j(s)}$ Basis.

Es gilt $s \geq 1$, denn sonst wäre $v_{n+1} \in L(v_1, \dots, v_n, v_{n+2}, \dots, v_r)$,

also wären $v_1, \dots, v_r$ linear abhängig ($\Rightarrow$ Lemma in 8.10) $\lightning$.

Aus der Induktionsvor. für $v_1, \dots, v_n, v_{n+2}, \dots, v_r, w_{j(1)}, \dots, w_{j(s)}$ und $w_1, \dots, w_k$

(hier ist immer noch $\#\{i \mid \dots\} = n$) folgt:

$$r - 1 + s \leq k.$$

Demnach gilt

$$r \overset{s \geq 1}{\leq} r - 1 + s \leq k.$$

□

8.12 Existenz von Basen

Satz: Jeder endlich erzeugte Vektorraum V besitzt eine Basis, und je zwei Basen haben die gleiche Länge.

Bew:

Existenz: V endlich erzeugt $\Rightarrow \exists w_1, \dots, w_k \in V : V = L(w_1, \dots, w_k)$.

Basisergänzungssatz (Satz 8.10) mit $r = 0$ zeigt:

$\exists j(1), \dots, j(s) :$ $w_{j(1)}, \dots, w_{j(s)}$ ist eine Basis.

Eindeutigkeit der Länge: Sind $v_1, \dots, v_r$ und $v_1', \dots, v_s'$ Basen, so liefert der Zusatz 8.11 zum Basisergänzungssatz (mit $w_j = v_j'$):

$$r \leq s$$

und Vertauschen der beiden Basen liefert ebenso $s \leq r$. $\square$

8.13 Dimension

Def: Die **Dimension** eines endlich erzeugten Vektorraums V ist die Länge einer (jeder) Basis.

Schreibweise: $\dim_K V \in \mathbb{N}$, oder $\dim V$ (falls K selbstverständlich ist).

Wir sagen, V hat **unendliche Dimension**, falls V nicht endlich erzeugt ist und schreiben: $\dim_K V = \infty$.

8.14 Weitere Konsequenzen aus dem Basisergänzungssatz

Korollar (= Folgerung) Sei V ein Vektorraum, $\dim V = n$.

1) Mehr als n Vektoren sind stets linear abhängig.
2) Weniger als n Vektoren erzeugen einen echten Unterraum: $L(v_1, \dots, v_r) \subsetneq V$ ($r < n \Rightarrow$)
3) Jedes linear unabhängige n-Tupel von Vektoren aus V ist eine Basis.
4) " n V erzeugende " " " "
5) Jedes maximal linear unabhängige System von Vektoren ist eine Basis.
6) " n minimale Erzeugendensystem " "
7) $V \cong K^n$
8) $K^n \cong K^m \iff n = m$.

Bew: Sei $u_1, \dots, u_n$ eine Basis von V.

1) $v_1, \dots, v_r$ linear unabhängig $\Rightarrow r \le n$. (Setze $w_i = u_i$ in Satz 8.10/8.11)
2) $V = L(w_1, \dots, w_k)$ $\Rightarrow n \le k$. (Setze $v_i = u_i$)
3) $v_1, \dots, v_n$ linear unabhängig.
   Wende Satz 8.10 an mit $w_i = u_i$ $\Rightarrow s = 0$, d.h. $v_1, \dots, v_n$ ist bereits eine Basis.
4) $V = L(w_1, \dots, w_n)$.
   Wende Satz 8.10 an mit $r = 0$ $\overset{\text{Satz 8.12}}{\Rightarrow} s = n$, d.h. $w_1, \dots, w_n$ ist bereits eine Basis.

5) $v_1, \dots, v_r$ lin. unabh. $\overset{\text{Satz 8.10 mit } w_i = u_i}{\Longrightarrow}$ $\exists\, j(1), \dots, j(s) : v_1, \dots, v_r, w_{j(1)}, \dots, w_{j(s)}$ Basis.

Aber $v_1, \dots, v_r$ ist bereits maximal linear unabhängig $\Rightarrow s = 0$. (und $r = n$)

6) $w_1, \dots, w_n$ Erzeugen $\overset{\text{Satz 8.10 mit } r = 0}{\Longrightarrow}$ $\exists\, j(1), \dots, j(s) : w_{j(1)}, \dots, w_{j(s)}$ Basis.

Aber $w_1, \dots, w_n$ ist bereits minimales Erzeugendensystem $\Rightarrow s = n$.

7) $\varphi : K^n \longrightarrow V$, $e_i \longmapsto u_i$ ist ein Isomorphismus ($\nearrow$ 8.8).

8) $n = \dim K^n = \dim K^m = m$.

8.15 Definition linearer Abbildungen durch Basen

Satz: Seien V, W K-Vektorräume und $v_1, \dots, v_n$ eine Basis von V.
Sind $w_1, \dots, w_n \in W$, so gibt es genau eine lineare Abbildung

$$\varphi : V \longrightarrow W$$

mit $\varphi(v_i) = w_i$, $i = 1, \dots, n$.

Bew: Ist $v \in V$, so gibt es eindeutige $\lambda_1, \dots, \lambda_n \in K$ mit $v = \sum_{i=1}^{n} \lambda_i v_i$. ($\nearrow$ Satz 8.4)

Wir müssen definieren: $\varphi(v) := \sum_{i=1}^{n} \lambda_i w_i$ [denn $\varphi(\sum \lambda_i v_i) \overset{!}{=} \sum \lambda_i \varphi(v_i)$]

Linearität: Sei $v = \sum_{i=1}^{n} \lambda_i v_i$, $w = \sum_{i=1}^{n} \mu_i v_i$ und $\lambda, \mu \in K$.

Dann gilt $\lambda v + \mu w = \sum_{i=1}^{n} (\lambda \lambda_i + \mu \mu_i) v_i$ und es folgt

$$\varphi(\lambda v + \mu w) = \sum_{i=1}^{n} (\lambda \lambda_i + \mu \mu_i) w_i = \lambda \cdot \Big(\sum_{i=1}^{n} \lambda_i w_i\Big) + \mu \cdot \Big(\sum_{i=1}^{n} \mu_i w_i\Big) = \lambda \varphi(v) + \mu \varphi(w).$$

□